$mathbb{F}_q$上の強正則グラフとアソシエーションスキームの構成法 (有限群とその表現,頂点作用素代数,代数的組合せ論の研究)

AUTHOR(S):

籾原, 幸二

CITATION:

籾原, 幸二. $mathbb{F}_q$上の強正則グラフとアソシエーションスキームの構成法 (有限群とその表現,頂点作用素代数,代数的組合せ論の研究). 数理解析研究所講究録 2014, 1872: 49-58

ISSUE DATE:

2014-01

URL:

http://hdl.handle.net/2433/195493

数理解析研究所講究録
第1872巻 2014年 49-58

Lifting construction of strongly regular graphs and association schemes in $\mathbb{F}_q$

– $\mathbb{F}_q$ 上の強正則グラフとアソシエーションスキームの構成法 –

熊本大学・教育学部数学科　　籾原　幸二*
Koji Momihara
Department of Mathematics, Faculty of Education,
Kumamoto University

概 要

論文 [8] の中で, 有限体 $\mathbb{F}_q$ 上の二次形式を用いた強正則ケーリーグラフおよびアソシエーション (トランスレーション) スキームの構成法を与えた. その構成法では, $\mathbb{F}_{q^2}$ の指数 $q-1$ の乗法部分群のいくつかのコセットの和集合を連結集合とする, $\mathbb{F}_{q^2}$ 上の強正則ケーリーグラフおよびアソシエーション (トランスレーション) スキームの存在を仮定した. この論文では, そのような条件を満たす, 有限体上の強正則グラフと 3-クラスのアソシエーションスキームの構成法を与える. この論文は, 論文 [5, 8] の要約である.

キーワード: 強正則グラフ, アソシエーションスキーム, ガウス和

1 導入

この論文では, 位数 q の有限体 $\mathbb{F}_q$ 上のケーリーグラフ $Cay(\mathbb{F}_q, D_i)$ らによる $\mathbb{F}_q$ 上の完全グラフの分解を考え, どのようなうまい $D_i \subseteq \mathbb{F}_q$ $(1 \leq i \leq d)$ に対し, その分解がアソシエーションスキームを成すかを考えたい.

よく知られている事実として, 対称的な 2-クラスアソシエーションスキームと強正則グラフの存在性は同値で, アソシエーションスキームの各 relation が, 強正則グラフとなる. 例えば, よく知られたアソシエーション (トランスレーション) スキームとして, 有限体の乗法部分群とそのコセットらを relation とする円分 (cyclotomic) スキームはよく知られている. また, Paley グラフはパラメータ $(v,k,\lambda,\mu) = (4t+1, 2t, t-1, t)$ を持つ強正則グラフであり, 有限体の指数 2 の乗法部分群とそのコセットを relation とする 2-クラスアソシエーションスキームである.

[1]〒 860-8555, 熊本県熊本市黒髪 2-40-1, 熊本大学教育学部数学科, Email: momihara@educ.kumamoto-u.ac.jp
この研究は, 科学研究費補助金 (研究活動スタートアップ 23840032) の補助を受けています.

今後, p を素数, f を正整数, $q := p^f$, k を $q-1$ を割る正整数, γ を $\mathbb{F}_q$ の一つの原始根とする. また, $C_i^{(k,q)} = \gamma^i\langle\gamma^k\rangle$ $(0 \le i \le k-1)$ と表記する. これらのコセットを円分類と呼ぶことにする. Momihara-Xiang は論文 [8] の中で, 以下のようなアソシエーションスキームの構成法を与えた.

定理 1.1. *([8])* n を偶数とし, $Q : V = \mathbb{F}_q^n \to \mathbb{F}_q$ を非特異な二次形式とする. $q-1$ を割る自然数 k に対し, A_i, $1 \le i \le d$ を $\{0,1,\ldots,k-1\}$ の部分集合とし, $\mathbb{F}_{q^2}$ 上の完全グラフのケーリーグラフ $Cay(\mathbb{F}_q, \bigcup_{\ell\in A_i} C_\ell^{(k,q^2)})$, $1 \le i \le d$ による分割が, d-クラスアソシエーションスキームを成すと仮定する. このとき, $\mathbb{F}_q^n$ 上の完全グラフのケーリーグラフ $Cay(V, D_0 \setminus \{0\})$ と $Cay(V, D_{\bigcup_{\ell\in A_i} C_\ell^{(e,q)}})$, $1 \le i \le d$ による分割は $(d+1)$-クラスアソシエーションスキームを与える. ここで, $D_u = \{x \in V \mid Q(x) = u\}$ とし, また, $X \subseteq \mathbb{F}_q$ に対し $D_X = \sum_{x\in X} D_x$ と定める.

例えば, 自明な適用例として, $d = k$ とし, $\mathbb{F}_{q^2}$ 上の d-クラスの円分スキームを持ってくれば, $\mathbb{F}_q^n$ 上の $d+1$ クラスのアソシエーションスキームが得られる. しかし, 一般にはこの構成法の種となるアソシエーションスキームについて, 多くのことは知られていない. この論文では, この構成法の条件を満たす, つまり, $q-1$ を割る自然数 k を位数とする円分類の和集合を連結集合に持つ $\mathbb{F}_{q^2}$ 上のアソシエーションスキームの構成法を与える. 特に, $d = 2$ および $d = 3$ の場合について扱う.

2 ガウス和および強正則グラフ・アソシエーションスキームに関する準備

2.1 準備

$\mathbb{F}_q$ の標準加法的指標 ψ と $\mathbb{F}_q$ のある乗法的指標 χ に対し, 指標和

$$G_f(\chi) = \sum_{x\in\mathbb{F}_q^*} \chi(x)\psi(x)$$

をガウス和と呼ぶ. ここでは, 以下のガウス和の計算に関するよく知られた性質を用いる.

(i) χ が非自明のとき, $G_f(\chi)\overline{G_f(\chi)} = q$.

(ii) p を $\mathbb{F}_q$ の標数とする. このとき, $G_f(\chi^p) = G_f(\chi)$.

(iii) $G_f(\chi^{-1}) = \chi(-1)\overline{G_f(\chi)}$.

(iv) χ が自明のとき, $G_f(\chi) = -1$.

(v) $\sigma_{a,b}(G_f(\chi)) = \chi^{-a}(b)G_f(\chi^a)$. ここで, k を χ の位数とし, $\sigma_{a,b}$ を $\gcd(a,k) = \gcd(b,p) = 1$ に対し, $\sigma_{a,b}(\zeta_k) = \zeta_k^a$ かつ $\sigma_{a,b}(\zeta_p) = \zeta_p^b$ で決まる $\mathbb{Q}(\zeta_{kp})$ の自己同型とする.

これまで, 小さな位数 k に対し, ガウス和の計算が行われてきた. 例えば, 位数 2 の場合のガウス和の計算は古くから知られている. また, 準原始的な場合 (すなわち $-1 \in \langle p\rangle \le (\mathbb{Z}/k\mathbb{Z})^*$ な

る場合) に対しても, ガウス和の値は完全に決定されており, また, これらの計算に基づいて様々な組合せ構造の存在性が示されてきた. 様々な結果および歴史については, [2] を参照されたい. 一方, 最近活発に研究されているケースは, 指数 e 型と呼ばれるケースであり, 以下のようなものである: $e = [(\mathbb{Z}/k\mathbb{Z})^* : \langle p \rangle]$ とする. また, p の $\mathbb{Z}/k\mathbb{Z}$ における位数 $\phi(k)/e$ を f と書く. この f に対し, $\mathbb{F}_{p^f}$ 上のガウス和 $G_f(\chi_k)$ を指数 e 型と呼ぶ. ここで, χ_k は $\mathbb{F}_{p^f}$ の位数 k の乗法的指標とする. 特に, $e = 2$ の場合は, このガウス和は完全に値が決定している ([11]). しかしながら, これら以外の場合における完全な計算結果はあまり知られておらず, 計算は容易でないように思われる.

以下は代数的グラフ理論でよく知られた結果である [3].

補題 2.1. $(G, +)$ を有限可換群とし, D を $0 \notin D$ かつ $D = -D$ を満たす G の部分集合とする. このとき,

$$\{\psi(D) \mid \psi \in \widehat{G}\}$$

が $Cay(G, D)$ の固有値全体を与える. ここで, $\widehat{G}$ は G の指標群とする.

一方で, 非自明な正則グラフが強正則であるための必要十分条件は, そのグラフの固有値がちょうど 3 つとなることが知られている [3]. (うち 1 つはグラフの次数である.) よって, $D = \bigcup_{i \in I} C_i^{(k,q)} \subseteq \mathbb{F}_q$ に対し, $Cay(\mathbb{F}_q, D)$ が強正則グラフを成すか否かは, $\psi(aD) = \sum_{x \in D} \psi(ax)$, $a \in \mathbb{F}_q^*$ がちょうど 2 つの値を取ることを示せばよい. ただし, ψ は $\mathbb{F}_q$ の標準加法的指標とする. また, $R_1, R_2, R_3 \subseteq \mathbb{F}_q^*$ を $R_i = -R_i$ を満たす $\mathbb{F}_q^*$ を分割する部分集合とするとき, $Cay(\mathbb{F}_q, R_i)$, $1 \leq i \leq 3$ が 3-クラスアソシエーションスキームを成すための必要十分条件は, 部分集合 $D_1, D_2, D_3 \subseteq \mathbb{F}_q^*$ で $\mathbb{F}_q^*$ を分割するものが存在し, $\psi(aR_i)$ の値が $a \in D_j$ なる j のみに依存することである.

ところで, 指標の直交性を用いて, $\psi(aD)$ はガウス和の言葉で以下のように表せる (cf. [6]):

$$\psi(aD) = \frac{1}{k} \sum_{\chi \in C_0^\perp} G_f(\chi^{-1}) \sum_{i \in I} \chi(a\gamma^i). \tag{2.1}$$

ここで, $C_0^\perp$ は $\widehat{\mathbb{F}_q^*}$ の部分群で, $C_0^{(k,q)}$ 上自明な乗法的指標から成る. よって, 強正則グラフの場合も, 3-クラスアソシエーションスキームの場合も本質的な計算は, ガウス和の計算が重要である. しかしながら, 既に述べたように, ガウス和の完全な計算を行うことは大変困難であるため, 可能な限りガウス和の直接的な計算を避けながら, 証明を行いたい. そこで, 我々は, 以下の Davenport-Hasse のリフトの公式と呼ばれる定理を用いる.

定理 2.2. *([2])* χ を $\mathbb{F}_q = \mathbb{F}_{p^f}$ の乗法的指標, χ' を χ の $\mathbb{F}_{q'} = \mathbb{F}_{p^{fs}}$ へのリフトとする. つまり, $\alpha \in \mathbb{F}_{q'}$ に対し, $\chi'(\alpha) = \chi(\mathrm{Norm}_{q'/q}(\alpha))$ と定める. このとき,

$$G_{fs}(\chi') = (-1)^{s-1}(G_f(\chi))^s$$

が成立する.

3 $\mathbb{F}_q$ 上の円分的強正則グラフから得られる $\mathbb{F}_{q^2}$ 上の強正則グラフ

この章では, 円分的強正則グラフと呼ばれる $\mathbb{F}_q$ 上の特別な強正則グラフを利用した, 強正則グラフの構成法を与える.

$\mathbb{F}_q$ の乗法部分群 D に対し, $Cay(\mathbb{F}_q, D)$ が強正則であれば, このグラフを円分的であるとよぶ. 円分的強正則グラフの存在性について以下の予想が知られている.

予想 3.1. *([9])* k を $k \mid \frac{p^f-1}{p-1}$ を満たす正整数とし, $C_0^{(k,p^f)} = -C_0^{(k,p^f)}$ を仮定する. このとき, $Cay(\mathbb{F}_{p^f}, C_0^{(k,p^f)})$ は以下のいずれかである.

(1) *(部分体型)* $d \mid f$ なる d に対し, $C_0^{(k,p^f)} = \mathbb{F}_{p^d}^*$,

(2) *(準原始型)* $-1 \in \langle p \rangle \leq (\mathbb{Z}/k\mathbb{Z})^*$,

(3) *(散在型)* $Cay(\mathbb{F}_{p^f}, C_0^{(k,p^f)})$ は表 *1* の *11* 個のいずれか.

表 1: 11 個の散在型

No.	k	p	f	$e := [(\mathbb{Z}/k\mathbb{Z})^* : \langle p \rangle]$
1	11	3	5	2
2	19	5	9	2
3	35	3	12	2
4	37	7	9	4
5	43	11	7	6
6	67	17	33	2
7	107	3	53	2
8	133	5	18	6
9	163	41	81	2
10	323	3	144	2
11	499	5	249	2

$\mathbb{F}_q$ とその m 次拡大 $\mathbb{F}_{q^m}$ を考え, L を $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$ の代表系とする. ここで, L の元として, $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x) = 0$ または 1 となるように選ぶことができる. ここで,

$$L_0 = \{x \in L \mid \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x) = 0\}, \quad L_1 = \{x \in L \mid \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x) = 1\}.$$

とおく. このとき,

$$H_0 = \{\overline{x} \in \mathbb{F}_{q^m}^*/\mathbb{F}_q^* \mid x \in L_0\} \tag{3.1}$$

は $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$ 上差集合を成す. (Singer 差集合と呼ばれている.) $\mathbb{F}_{q^m}^*$ の位数 $(q^m-1)/(q-1)$ の乗法的指標 χ は, $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$ の指標を誘導する. このとき, 山本 [10] の結果より, $\chi(H_0) = G_{fm}(\chi)/q$ が成立する.

$\mathbb{F}_q^* \leq C_0(:=C_0^{(k,q^m)}) \leq \mathbb{F}_{q^m}^*$ なる部分群 C_0 に対し, $\overline{C_0} = C_0/\mathbb{F}_q^* \leq \mathbb{F}_{q^m}^*/\mathbb{F}_q^*$ とおく. また, S を $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$ を $\overline{C_0}$ で割った剰余群の代表系とし, $G = \{\overline{s} \,|\, s \in S\} \simeq \mathbb{F}_{q^m}^*/C_0$ とする.

今, $Cay(\mathbb{F}_{q^m}, C_0)$ が強正則であると仮定する. このとき, $|H_0 \cap s\overline{C_0}|$, $s \in S$ はちょうど 2 つの値を取る [4, 9]. よって, $|H_0 \cap s\overline{C_0}| - |H_0 \cap \overline{C_0}| = 0, \delta$ を得る. ここで, δ は非零整数である. 今, χ_0 を $\mathbb{F}_{q^m}$ の自明な乗法的指標とし, χ を $\chi^k = \chi_0$ なる任意の指標とする. このとき,

$$\begin{aligned}\chi(H_0) &= \sum_{s\in S} |H_0 \cap s\overline{C_0}|\chi(\overline{s}) \\ &= \sum_{s\in S} (|H_0 \cap s\overline{C_0}| - |H_0 \cap \overline{C_0}|)\chi(\overline{s}) \\ &= \delta \sum_{s\in S'} \chi(\overline{s})\end{aligned}$$

を得る. ここで,

$$S' = \{s \in S : |H_0 \cap s\overline{C_0}| - |H_0 \cap \overline{C_0}| = \delta\} \tag{3.2}$$

とする. よって, 以下の公式を得る.

$$\sum_{s\in S'} \chi(\overline{s}) = \frac{\chi(H_0)}{\delta} = \frac{G_{fm}(\chi)}{\delta q}. \tag{3.3}$$

注意 3.2. δ は p の冪であり, また, $\overline{S'} := \{\overline{s} \mid s \in S'\} \subset G$ は G 上 $(k, |S'|, \lambda')$ 差集合を成す. H_0 の部分差集合と呼ばれる.

γ を $\mathbb{F}_{q^{2m}}$ の原始根, $\omega = \mathrm{Norm}_{q^{2m}/q^m}(\gamma) = \gamma^{q^m+1}$ とすると, ω は $\mathbb{F}_{q^{2m}}$ の部分体 $\mathbb{F}_{q^m}$ の原始根である. また, $C_j^{(k,q^{2m})} = \gamma^j\langle\gamma^k\rangle$, $C_j^{(k,q^m)} = \omega^j\langle\omega^k\rangle = \omega^j C_0$ とおく.

定理 3.3. $\mathbb{F}_q^* \leq C_0 \leq \mathbb{F}_{q^m}^*$ を $[\mathbb{F}_{q^m}^* : C_0] = k$ かつ $-C_0 = C_0$ を満たす部分群とし, $Cay(\mathbb{F}_{q^m}, C_0)$ が円分的強正則グラフであると仮定する. 今, $I = \{0 \leq i \leq k-1 \mid \overline{\omega^i} \in S'\}$ と定める. ここで, S' は *(3.2)* で定義された S の部分集合とし, $\overline{\omega}$ は, $\omega\mathbb{F}_q^*$ を意味するものとする. このとき, $D = \bigcup_{i\in I} C_i^{(k,q^{2m})}$ とすると , $Cay(\mathbb{F}_{q^{2m}}, D)$ は強正則である.

証明: ψ_1 を $\mathbb{F}_{q^{2m}}$ の標準加法的指標とし, χ_k' を $\mathbb{F}_{q^{2m}}$ の位数 k の乗法的指標とする. $Cay(\mathbb{F}_{q^{2m}}, D)$ の次数以外の固有値は $\psi_1(\gamma^a D)$, $0 \leq a \leq k-1$ で与えられることに注意し, $Cay(\mathbb{F}_{q^{2m}}, D)$ が強正則であることを示すために,

$$T_a = k \cdot \psi_1(\gamma^a D) + |I| = \sum_{x=1}^{k-1} G_{2fm}(\chi_k'^{-x}) \sum_{i\in I} \chi_k'^x(\gamma^{a+i})$$

を $a = 0, 1, \ldots, k-1$ のすべてで計算する必要がある. $k \,|\, (q^m - 1)$ に対し, χ_k' は $\mathbb{F}_{q^m}$ のある指標 χ_k のリフトであることに注意し, Davenport-Hasse のリフトの公式から

$$T_a = -\sum_{x=1}^{k-1} {\chi_k}^x(\omega^a) G_{fm}(\chi_k^{-x}) G_{fm}(\chi_k^{-x}) \sum_{i\in I} \chi_k^x(\omega^i)$$

を得る. また, I の定義より,

$$\sum_{i\in I}\chi_k^x(\omega^i)=\sum_{s\in S'}\chi_k^x(s)=\frac{G_{fm}(\chi_k^x)}{\delta q}$$

を得る. よって,

$$\begin{aligned}T_a &= -\frac{1}{\delta q}\sum_{x=1}^{k-1}\chi_k^x(\omega^a)G_{fm}(\chi_k^{-x})G_{fm}(\chi_k^{-x})G_{fm}(\chi_k^x)\\ &= -\frac{q^{m-1}}{\delta}\sum_{x=1}^{k-1}\chi_k^x(\omega^a)G_{fm}(\chi_k^{-x}),\end{aligned}\tag{3.4}$$

が成立する. 最後に, 仮定から $Cay(\mathbb{F}_{q^m},C_0^{(k,q^m)})$ は強正則より, $\sum_{x=1}^{k-1}\chi_k^x(\omega^a)G_{fm}(\chi_e^{-k})$, $a=0,1,\ldots,k-1$ はちょうど 2 つの値を持つ. すなわち, T_a, $0\le a\le k-1$ は 2 つの値を持ち, よって, $Cay(\mathbb{F}_{q^{2m}},D)$ は強正則である. □

定理の部分集合 D の濃度は $|D|=\frac{(q^m-1)}{k}|I|(q^m+1)$ である. 今, 既知の円分的強正則グラフに定理を適用して, 以下の 3 つの系を得ることができる. 以下の系はそれぞれ, 準原始型, 部分体型, 散在型に対応している.

系 3.4. p を素数, $q^m=p^{2jr}$, $k\,|\,(p^j+1)$ とし, j はこの条件を満たす最小の正整数とする. このとき, $n=q^m$ と $r=(q^m-1)/k$ に対し, $(n^2,r(n+1),-n+r^2+3r,r^2+r)$-強正則グラフが存在する.

系 3.5. q を素数冪, $m\ge 3$, a を m の任意の因数とする. このとき, $n=q^m$ と $r=q^{m-a}-1$ に対し, $(n^2,r(n+1),-n+r^2+3r,r^2+r)$-強正則グラフが存在する.

系 3.6. (q,k,e) を以下の 11 個のいづれかとする.

$$\begin{aligned}(q,k,e) &= (3^5,11,5),(5^9,19,9),(3^{12},35,17),(7^9,37,9),(11^7,43,21),(17^{33},67,33)\\ &\quad (3^{53},107,53),(5^{18},133,33),(41^{81},163,81),(3^{144},323,161),(5^{249},499,249).\end{aligned}$$

このとき, $(q^2,r(q+1),-q+r^2+3r,r^2+r)$-強正則グラフが存在する. ここで, $r=e(q-1)/k$ とする.

4 $\mathbb{F}_{2^{6s}}$ 上の 3-クラスアソシエーションスキーム

この章では, $\mathbb{F}_{2^{6s}}$ 上の 3-クラスアソシエーションスキームの構成法を与える.

4.1 $\mathbb{Z}_{\frac{2^{3s}-1}{2^s-1}}$ の分割

s を正整数, $k=\frac{2^{3s}-1}{2^s-1}$ とし, $F:=\mathbb{F}_{2^{3s}}$, $E:=\mathbb{F}_{2^s}$ とおく. さらに,

$$D:=\{u\in F^*\,|\,\mathrm{Tr}_{F/E}(u^{-1})=0\}\tag{4.1}$$

とする. この集合 D は, $g \in E^*$ に対し, $Dg = \{dg \mid d \in D\} = D$ を満たすので, $\psi(\omega^a D)$ の値は, $a \pmod k$ で決まる. (ω は F の原始根.) いま, $\psi(\omega^a D)$, $0 \le a \le k-1$ が 3 つの値を持つことを示す. 加法的指標の定義より, 以下を得る.

$$\begin{aligned}\psi(\omega^a D) &= \frac{1}{2^s-1}\sum_{u\in D}\sum_{x\in E^*}\psi(x\omega^a u)\\ &= |\{u \mid u \in D, \mathrm{Tr}_{F/E}(\omega^a u) = 0\}| - \frac{1}{2^s-1}|\{u \mid u \in D, \mathrm{Tr}_{F/E}(\omega^a u) \neq 0\}|\\ &= -(2^s+1) + \frac{2^s}{2^s-1}|\{u \mid u \in D, \mathrm{Tr}_{F/E}(\omega^a u) = 0\}|.\end{aligned}$$

ここで, $u^{\frac{2^{3s}-1}{2^s-1}}\mathrm{Tr}_{F/E}(u^{-1}) = \mathrm{Tr}_{F/E}(u^{1+2^s})$ より,

$$D = \{u \in F^* \mid \mathrm{Tr}_{F/E}(u^{1+2^s}) = 0\}$$

を得る. 一方, $Q(x) = \mathrm{Tr}_{F/E}(x^{1+2^s})$ は, E 上の非退化な二次形式より, 対応する $PG(2,2^s)$ の二次曲線 $\mathcal{Q}$ は $PG(2,2^s)$ の各直線と以下のように交差する [7].

$$\begin{cases} 2^s+1 \text{ 本の直線は } 1 \text{ 点で交差,} \\ 2^{2s-1}+2^{s-1} \text{ 本の直線は } 2 \text{ 点で交差,} \\ 2^{2s-1}-2^{s-1} \text{ 本の直線は交差なし.} \end{cases}$$

ここで, $\mathrm{Tr}_{F/E}(a) = 0$ なる $a \neq 0$ に対し,

$$L_a = \{[x] \mid x \in F^*, \mathrm{Tr}_{F/E}(ax) = 0\}$$

は直線を与えるので ($[x]$ は $x \in F^*$ に対し, $x \cdot E^*$ に対応する $PG(2,2^s)$ の点とする)[1], 集合

$$S_a := \{u \mid \mathrm{Tr}_{F/E}(u^{1+2^s}) = 0, \mathrm{Tr}_{F/E}(\omega^a u) = 0\}$$

の濃度は, $0, 2^s-1, 2(2^s-1)$ のいずれかとなる. 今,

$$T_i = \{a \in \mathbb{Z}_k : |S_a| = i\cdot(2^s-1)\},\ i = 0,1,2$$

とする. このとき, 明らかに $|T_0| = 2^{2s-1}-2^{s-1}$, $|T_1| = 2^s+1$, $|T_2| = 2^{2s-1}+2^{s-1}$ が成立する. よって, 以下の補題を得る.

補題 4.1. $\psi(\omega^a D)$, $0 \le a \le k-1$ はちょうど 3 つの値をもち, それらは

$$\psi(\omega^a D) = \begin{cases} -2^s-1 & \text{if } a \in T_0 \\ -1 & \text{if } a \in T_1, \\ 2^s-1 & \text{if } a \in T_2. \end{cases}$$

で与えられる.

さらに以下の補題を得る. (証明は [5] を参照されたい.)

補題 4.2. 各 T_i を群環 $\mathbb{Z}[\mathbb{Z}_k]$ の元と同一視するものとする．このとき，以下が成立する．

$$(T_2 - T_0)T_1^{(-1)} = 2^s T_1, \tag{4.2}$$

$$(T_2 - T_0)T_2^{(-1)} = 2^{2s-1} + 2^{s-1}(\mathbb{Z}_k - T_1), \tag{4.3}$$

$$(T_2 - T_0)T_0^{(-1)} = -2^{2s-1} + 2^{s-1}(\mathbb{Z}_k - T_1). \tag{4.4}$$

注意 4.3. 今，T_1 は

$$T_1 = \{i \in \mathbb{Z}_k : |\operatorname{Tr}_{F/E}(w^i) = 0\}$$

で与えられ，$\mathbb{Z}_k$ 上差集合を成すので，$T_1 T_1^{(-1)} = 2^s + \mathbb{Z}_k$ が成立することに注意する．

4.2 $\mathbb{F}_{2^{6s}}$ 上の 3-クラスアソシエーションスキーム

T_0, T_1, T_2 は前章の通りとし，$G := \mathbb{F}_{2^{6s}}$ とおく．$C_i^{(k,2^{6s})}$, $0 \le i \le k-1$ を G の位数 k の円分類とする．ψ, ψ' をそれぞれ F and G の標準加法的指標とする．また，G の原始根 γ に対し，

$$\omega = \operatorname{Norm}_{G/F}(\gamma),$$

とおくと，これは F の原始根である．

以下がこの章の主定理である．

定理 4.4. G の以下の分割を考える．

$$R_0 = \{0\},\ R_1 = \bigcup_{i \in T_1} C_i^{(k,2^{6s})},\ R_2 = \bigcup_{i \in T_2} C_i^{(k,2^{6s})},\ R_3 = \bigcup_{i \in T_0} C_i^{(k,2^{6s})}.$$

このとき，$(G, \{R_i\}_{i=0}^3)$ は 3-クラスアソシエーションスキームを成す．

証明: G の指数 k の任意の乗法的指標 χ' に対し，F の指標 χ が存在し，χ' は χ のリフトとみなせる．今，$\eta'_a = \psi'(\gamma^a C_0^{(k,2^{6s})})$, $0 \le a \le k-1$ の値を計算する．Davenport-Hasse のリフトの公式と $G_{3s}(\chi) = 2^s \sum_{x \in T_1} \chi(\gamma^x)$ より，

$$\begin{aligned}
\eta'_a &= \frac{1}{k}\sum_{\ell=0}^{k-1} G_{6s}(\chi'^{-\ell})\chi'^{\ell}(\gamma^a) \\
&= -\frac{1}{k} + \frac{-1}{k}\sum_{\ell=1}^{k-1} G_{3s}(\chi^{-\ell})^2 \chi^{\ell}(\omega^a) \\
&= -\frac{1}{k} + \frac{-2^s}{k}\sum_{\ell=1}^{k-1} G_{3s}(\chi^{-\ell}) \sum_{i \in T_1} \chi^{\ell}(\omega^{a-i}) \\
&= -\frac{1}{k} + \frac{-2^s}{k}\left(\sum_{\ell=0}^{k-1} G_{3s}(\chi^{-\ell}) \sum_{i \in T_1} \chi^{\ell}(\omega^{a-i}) + 2^s + 1\right) \\
&= -2^s \psi(\omega^a D) - 1
\end{aligned}$$

表 2: $\psi'(\gamma^a R_h)$ の値 ($(G, \{R_i\}_{i=0}^3)$ の指標表)

	R_0	R_1	R_2	R_3
$\gamma^a = 0$	1	$(2^{2s}-1)(2^{3s}+1)$	$2^{s-1}(2^{2s}-1)(2^{3s}+1)$	$2^{s-1}(2^s-1)^2(2^{3s}+1)$
$a = 0$	1	$2^{2s}-1$	$2^{s-1}(2^s+1)(-2^{2s}+2^s-1)$	$2^{s-1}(2^s-1)(2^{2s}+2^s-1)$
$a \in T_1$	1	$-2^{3s}+2^{2s}-1$	$2^{s-1}(2^{2s}-1)$	$2^{s-1}(2^s-1)^2$
$a \notin T_1 \cup \{0\}$	1	$2^{2s}-1$	-2^{s-1}	$2^{s-1}(-2^{s+1}+1)$

表 3: $\psi'(\gamma^a D_h)$ の値 ($(G, \{D_i\}_{i=0}^3)$ の指標表)

	D_0	D_1	D_2	D_3
$\gamma^a = 0$	1	$(2^s-1)(2^{3s}+1)$	$(2^{2s}-1)(2^{3s}+1)$	$(2^{2s}-1)^2(2^{2s}-2^s+1)$
$a \in T_1$	1	2^s-1	$-2^{3s}+2^{2s}-1$	$(2^s-1)^2(2^s+1)$
$a \in T_2$	1	$-2^{2s}+2^s-1$	$2^{2s}-1$	-2^s+1
$a \in T_0$	1	$2^{2s}+2^s-1$	$2^{2s}-1$	$-(2^s+1)(2^{s+1}-1)$

を得る. ここで D は (4.1) で定義された集合である. 今, 補題 4.1 より,

$$\eta'_a = \begin{cases} 2^{2s}+2^s-1 & \text{if } a \in T_0, \\ 2^s-1 & \text{if } a \in T_1, \\ -2^{2s}+2^s-1 & \text{if } a \in T_2, \end{cases}$$

が得られる. 続いて, 目的であった $\psi'(\gamma^a R_h)$ の計算を行う.

$$\begin{aligned} \psi'(\gamma^a R_h) &= \sum_{i \in T_h} \eta'_{a+i} \\ &= (2^s-1)|T_1 \cap a + T_h| + (-2^{2s}+2^s-1)|T_2 \cap a + T_h| + (2^{2s}+2^s-1)|T_0 \cap a + T_h| \\ &= (2^s-1)|T_h| - 2^{2s}|T_2 \cap a + T_h| + 2^{2s}|T_0 \cap a + T_h|. \end{aligned}$$

ここで, $-2^{2s}|T_2 \cap a + T_h| + 2^{2s}|T_0 \cap a + T_h|$ の値は群環の元 $-2^{2s}(T_2 - T_0)T_h^{(-1)}$ における a の係数であることに注意し, 補題 4.2 より, $\psi'(\omega^a R_h)$ の値は表 2 のように計算できる. 特に,

$$D_0 = \{0\},\ D_1 = C_0^{(k,2^{6s})},\ D_2 = \cup_{i \in T_1} C_i^{(k,2^{6s})},\ D_3 = \cup_{i \in (T_0 \cup T_2) \setminus \{0\}} C_i^{(k,2^{6s})}. \tag{4.5}$$

とおくと, $\psi'(aR_i)$ の値が $a \in D_j$ なる j のみに依存しているので, $(G, \{R_i\}_{i=0}^3)$ は 3-クラスアソシエーションスキームである. □

注意 4.5. 定理で得られたアソシエーションスキームの双対スキームは, $(G, \{D_i\}_{i=0}^3)$ である. ここで, D_i は *(4.5)* で定められた集合である. このアソシエーションスキームの $\psi'(\gamma^a D_h)$ の値は表 *3* で与えられる.

参考文献

[1] K. T. Arasu, J. F. Dillon, D. Jungnickel, A. Pott, The solutions of the Waterloo problem, *J. Combin. Theory, Ser. A*, **71** (1995), 316–331.

[2] B. Berndt, R. Evans, K. S. Williams, *Gauss and Jacobi Sums*, Wiley, 1997.

[3] A. E. Brouwer, W. H. Haemers, *Spectra of Graphs*, course notes, available at `http://homepages.cwi.nl/~aeb/math/ipm.pdf`

[4] R. Calderbank, W. M. Kantor, The geometry of two-weight codes, *Bull. London Math. Soc.*, **18** (1986), 97–122.

[5] T. Feng, K. Momihara, Three-class association schemes from cyclotomy, ArXiv: 1211.2864.

[6] T. Feng, Q. Xiang, Strongly regular graphs from union of cyclotomic classes, to appear in *J. Combin. Theory, Ser. B.*

[7] R. A. Games, The geometry of quadrics and correlations of sequences, *IEEE Trans. Inform. Theory*, **32** (1986), 423–426.

[8] K. Momihara, Q. Xiang, Lifting constructions of strongly regular Cayley graphs, Arxiv: 1212.5752.

[9] B. Schmidt, C. White, All two-weight irreducible cyclic codes?, *Finite Fields Appl.*, **8** (2002), 321–367.

[10] K. Yamamoto, On Jacobi sums and difference sets, *J. Combin. Theory, Ser. A,* **3** (1967), 146–181.

[11] J. Yang, L. Xia, Complete solving of explicit evaluation of Gauss sums in the index 2 case, *Sci. China Ser. A*, **53** (2010), 2525–2542.